CSC-EPL-88/002

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF CORTANA SYSTEMS CORPORATION

CORTANA PERSONAL COMPUTER SECURITY SYSTEM Version 1.21

18 February 1988

SUB-SYSTEM EVALUATION REPORT

CORTANA SYSTEMS CORPORATION

CORTANA PERSONAL COMPUTER SECURITY SYSTEM

VERSION 1.21

NATIONAL COMPUTER SECURITY CENTER

9800 SAVAGE ROAD

FORT GEORGE G. MEADE MARYLAND 20755-6000

February 18, 1988

CSC-EPL-88/002
Library No. S230,456

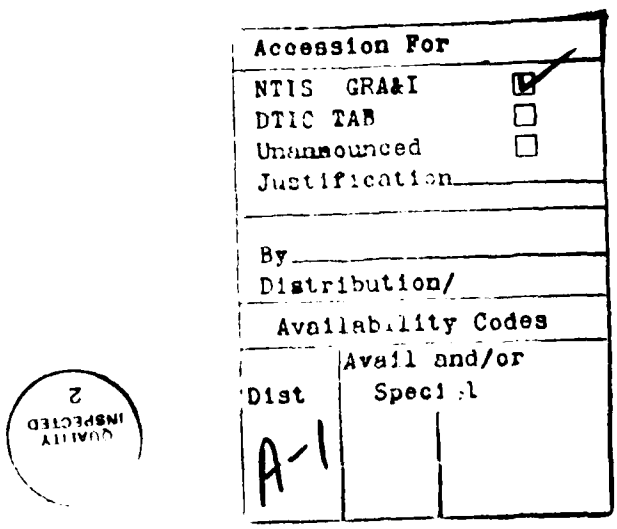
FOREWORD

This publication, the Sub-system Evaluation Report, Cortana Systems Corporation, Cortana Personal Computer Security System Version 1.21, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the evaluation of Cortana's Cortana Personal Computer Security System Version 1.21. The requirements stated in this report are taken from *Department of Defense Trusted Computer System Evaluation Criteria*, dated December 1985.

Approved:

February 18, 1988

Eliot Sohmer
Chief, Security Evaluations,
Publications, and Support,
National Computer Security Center



ACKNOWLEDGEMENTS

Evaluation Team Members

Stephen F. Carlton
Donald N. Dasher
John W. Taylor

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

TABLE OF CONTENTS

This page intentionally left blank.

EXECUTIVE SUMMARY

The Cortana Personal Computer Security System[1] Version 1.21 has been evaluated by the National Computer Security Center (NCSC). The Cortana Personal Computer Security System is considered to be a security sub-system rather than a complete trusted computer system. Therefore, it was evaluated against a relevant subset of the requirements in the *Department of Defense Trusted Computer System Evaluation Criteria* (TCSEC), dated December 1985. Specifically, the features included in this evaluation are Identification and Authentication (I&A), Discretionary Access Control (DAC), Object Reuse, and Audit.

The NCSC evaluation team has determined that the Cortana Personal Computer Security System may be capable of applying these security features to any IBM PC/AT or PC/XT[2] when configured with the appropriate restrictions.[3] The Cortana Personal Computer Security System maintains I&A by requiring that users identify themselves and provide authentication before gaining access to the computer. DAC is provided on individual user's files through the use of address translation. By supplying a utility that over-writes files, the object reuse mechanism gives assurance that data may not be able to be scavenged. In addition, the Cortana Personal Computer Security System provides the means to audit workstation activity, including attempts to violate the security of the system.

The security mechanisms provided can be trusted only if the code which implements them is protected from modification. This protection is difficult to implement in a computer system which only provides a single state of execution (e.g., a PC). The Cortana Personal Computer Security System does not provide a mechanism to protect its code from modification and is therefore open to possible security breaches. Through the use of certain utilities, a user may be able to access files to which the Cortana Personal Computer Security System provides protection.

---

(1) The Cortana Personal Computer Security System is a registered trademark of the Cortana Systems Corporation

(2) IBM PC/AT and PC/XT are registered trademarks of the International Business Machines Corporation.

(3) For a list of these restrictions, please refer to Section 3, "The Product in a Trusted Environment".

It is also possible to modify the Cortana Personal Computer Security System protection mechanisms and the underlying operating system.

To keep such utilities from being used on the system, the Cortana Personal Computer Security System must be configured such that each user is forced to use menus and is not able to access to system "C>" prompt. Such a configuration is difficult to implement and, when the appropriate restrictions are placed on the system, causes severe limitation in the number of applications able to run on the system.

Because of the Cortana Personal Computer Security System's protection scheme, it is easy to render the hard disk unusable. The Cortana Personal Computer Security System modifies the File Allocation Table (FAT) of the hard disk and performs address translation from the modification. Because of frequent crashes rendering the system useless, the team found this product difficult to test.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the TCSEC. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Sub-systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub-system evaluation is limited to consideration of the sub-system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub-system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would

violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

The Cortana Personal Computer Security System is an add-on security product which, when configured as tested on any IBM PC/XT or PC/AT, can provide user Identification and Authentication (I&A), Discretionary Access Control (DAC), Object Reuse, and Audit mechanisms.

The Cortana Personal Computer Security System is comprised of an expansion board and software utilities which provide the security mechanisms. These utilities are located on two floppy disks which are used to configure the workstation environment and to provide security mechanisms. Upon Cortana Personal Computer Security System installation, the product modifies the File Allocation Table of the Hard Disk and the utilities that provide the security mechanisms are copied to the hard disk. The System Administrator programs remain on the floppy disk to add physical protection. The System Administrator utilities provide functionality to define the commands each user is allowed to access. These utilities also provide a mechanism for setting variable system parameters parameters such as the duration of the audit log. The administrator is able to specify the commands that each individual user is allowed to use by explicitly securing them in the "Secured Functions" or "Secured Applications" lists. This separates, for each user, the privileged functions from the non-privileged functions.

The Cortana Personal Computer Security System provides for more than one System Administrator. The original System Administrator establishes the user and system environments and has the ability to designate secondary System Administrators. Also, the System Administrator is able to generate new system and user passwords.

Evaluation of Functionality

The team has determined that the Cortana Personal Computer Security System provides mechanisms for I&A, DAC, Object Reuse, and Audit of workstation activity. Each is described separately below.

Identification & Authentication

The Cortana Personal Computer Security System provides for I&A of the users of a workstation. When the workstation is Reset and the Cortana Personal Computer Security System has been configured to require a system password, the Cortana Personal Computer Security System prompts the Administrator for an ACCESS CODE. The administrator must enter the system password at this time. He will be given up to three chances to enter the password correctly. Failure to do so will cause the message "Security Breach" to be displayed and an audit record entry will be created. The

password is not displayed on the screen when being typed in. After the system password has been entered correctly, the administrator will be prompted for the time and date.

Following the boot procedure, the system prompt "C>" is displayed on the screen. A user wishing to gain access to the workstation enters the command "signon". This is the only command the system will recognize at this time. The user is then prompted for his identifier and password. The identifier is assigned to each user by the system administrator. The password is not displayed when typed in. If the information entered by the user is correct, the message *user name* signed on at *time and date* is displayed. Next, a menu which shows the applications or DOS functions that the user is permitted to use appears. The administrator may configure the system to provide the system prompt, applications menu, or secured functions menu at this time, depending on the access granted to the user.

The first time a user signs on to a workstation that has the Cortana Personal Computer Security System installed on it, the procedure is the same as above with one exception. When the user is prompted for his password he enters the initial password "newuser". The Cortana Personal Computer Security System then requires the user to change his password before being allowed to continue.

Discretionary Access Control

The Cortana Personal Computer Security System provides DAC on individual files and directories by allowing the administrator to specify who may access them. In addition, the administrator can configure the Cortana Personal Computer Security System to give the user custom menus that specify the files and directories to which he has access. It is important to note that the DAC provided by the Cortana Personal Computer Security System is not set by the user, but rather it is set by the administrator using the "secure functions" menu.

Object Reuse

Normally, when a file is deleted under PC-DOS, the contents of the file remain on the disk and may be recovered. The Cortana Personal Computer Security System provides the ability for users to write over a file before it is deleted by using the ZERO command. For a user to use this feature the administrator must have given the user access to this command in the secure functions list. In addition, the Cortana Personal Computer Security System clears all RAM when a user logs out to prevent him from leaving behind some data which could be scavenged.

Audit

The Cortana Personal Computer Security System provides the capability to create an audit log of workstation activity such as user signon, invalid signon, and user signoff. A complete list of the

events that are recorded can be found on pages 69-71 of the System Administrator's Manual. The audit records are kept in a file on the hard disk. The size of the audit file is limited by both the configuration parameter and the available disk space. When this file is exhausted, the Cortana Personal Computer Security System begins overwriting audit records beginning with the oldest. In addition, the Cortana Personal Computer Security System provides an audit reduction tool that allows easy processing and analysis of the audit data.

Evaluation of Documentation

The Cortana Personal Computer Security System System documentation consists of two guides, the System Administrator's Guide, 1986, and the General User's Guide, 1986. These two documents, described below, contain a detailed description of the security features provided by the Cortana Personal Computer Security System. The documentation assumes a minimal knowledge of computers.

System Administrator's Guide

This manual is intended for the individual responsible for installing the system and also for the System Administrator (SA). The following sections are included:

PREFACE

The preface lists the security features the Cortana Personal Computer Security System implements, the components of the Cortana Personal Computer Security System, and the hardware base required to use it.

INTRODUCTION

The introduction is split into two sections. The first section contains a complete overview of the Cortana Personal Computer Security System. The second gives a brief introduction on how to use the Cortana Personal Computer Security System.

Overview of the System

This section further explains each of the security features the Cortana Personal Computer Security System provides. It also introduces access control to individual files or groups of files. Finally, access to users is introduced and how these accesses are set.

Using the Security System

This section first discusses instructions on how to use this manual. It then describes the use of menus, boxes, and keys. Next, there is a brief tutorial on keeping an ideal secure environment followed by a step-by-step guide to signing on to a Cortana Personal Computer Security System.

SETTING UP A BASIC SYSTEM

This section gives the System Administrator an outline on how to set up the Cortana Personal Computer Security System for the first time.

TUTORIAL

This section gives the System Administrator a working example on how to execute the Cortana Personal Computer Security System to create a secure system. The tutorial gives basic instructions and a model to use for entering information. Such tasks as adding users to the system, creating directories, assigning ownership to those directories, assigning access to those directories, deleting users, and deleting directories are given in work-through examples.

THE CORTANA ADMINISTRATOR'S PROGRAM

This section deals with the SA's program. The program can be executed only by the designated system administrator. The program is contained on a separate diskette that should be in the SA's possession.

Starting the program

This section shows how to begin use of the security system and how to get the programs running.

User environment

This section describes one of five menus available to the SA. Within this menu are five sub-menus: declare directories, secured functions, menu generation, applications, and user definition. This section describes the function of each of these sub-menus. The "declare directories" section describes how to check on or change the status -

whether public or private - of all directories on the system. The "secured function" section describes how to secure, change or delete the name of a function whose use the SA wishes to regulate. A function in the Cortana Personal Computer Security System is the user of a program, data file, or a DOS command. The "menu generation" section details how to generate an application or DOS menu for your users and to restrict (or allow) the system prompt. The section on applications states how to add, change, or delete the name of an application from the list of applications. Also, how to restrict the use of applications is outlined, here. The section on user definition describes how to add, change, delete, or suspend users or to set the access for a specific user.

System environment

This is another menu available to the SA. Within this menu are three sub-menus: de-install , change system setup, and restore system. The de-install section talks about how, when, and why to de-install the Cortana Personal Computer Security System. The section on change system setup tells how to set or change parameters in the overall Cortana Personal Computer Security System setup that have to do with recording computer activity, setting user identification length, logging off an unused system after a certain period of time, and writing a message to your users. The restore system section describes how to restore the Cortana Personal Computer Security System to the hard disk.

Reports Menu

This is the third menu the SA can go into. Within this menu are two sub-menus: print report and clear history (audit) file. The print report portion details how to print reports of the activity on the Cortana Personal Computer Security System. The clear history file part tells how to clear old information on your history files.

Generate new passwords

This is the fourth menu selection the SA has and this section describes how to generate new passwords.

Quit

This section briefly describes how to quit the System Administrator's Program.

REFERENCE

This section gives the SA a quick reference for any function help is needed on. The topics an SA can reference here are: activity logging and reports, automatic execution of batch files, clock systems, command processor, user commands, SA commands, software installation, hardware installations, updating, passwords and identification, special applications, substitute commands, terminate and stay resident programs, and utility and diagnostic programs.

GLOSSARY

The SA guide provides a glossary of terms that relate to the hardware and the security system for quick reference.

APPENDIX: CORTANA SYSTEM FLOWCHART

The SA guide provides a system wire chart showing the menus, sub-menu's, and actions able to be performed from each menu.

INDEX

The SA guide provides a referencing index.

General User's Guide

This manual is intended for the Cortana Personal Computer Security System general user (e.g., one without SA privileges). It provides instruction on basic usage of the product and overlaps with the System Administrator's Guide in this area.

INTRODUCTION

The introduction gives a brief summary of the Cortana Personal Computer Security System and proposes that the user know who the SA is and keep his password confidential.

SIGNING ON TO A CORTANA SECURED SYSTEM

This section is broken into three parts to simplify the procedure for the inexperienced user. The three parts are the start or boot signon, the system signon, and the signing on for the first time.

The startup or boot signon

In this part the procedure to boot the Cortana Personal Computer Security System is explained and what is to be done should problems arise.

The system signon

This section describes to the user how to access the capabilities of his computer through the Cortana Personal Computer Security System. Here is where the Identification and Authentication of users is explained.

Signing on for the first time

In this section, the procedures for acquiring a password for the first time are described.

COMMANDS

This section presents the commands to the user. The user or the SA can determine the characteristics of the Cortana Personal Computer Security System and enter or exit the system. Again, this is explained in two sections, the user commands from the system prompt and user commands from a custom menu.

User commands from the system prompt

In this section, a list of commands and an explanation of those commands are presented to the user. All actions taken by the system are posted for the user to see what will happen given the execution of any given command.

User commands from a custom menu

The user is given a list of commands that can be applied to an applications menu or DOS menu. These commands have been embedded in function keys and the operation of them is briefly explained.

SPECIAL USES

This section describes how a user can use the custom menus (both the applications and DOS menus) and perform automatic execution of batch files.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it an increased need to protect and control access to data stored on these systems. Initially, protection was provided mainly by the individual user having physical possession of his own data and operating system on diskettes, resulting in a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users' data, thus preventing intentional or accidental access to other users' data. Other security mechanisms were not deemed necessary since the user was only able to inflict damage to his own data or operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In a working environment where it was common to have several users share the same workstation, they now share and store their data on the same hard disk memory unit. In this environment, users no longer have the assurance that their data is protected from unauthorized access, or even that the underlying operating system has not been subverted. Procedural controls no longer provide adequate users' data isolation and control necessary for this environment.

The Cortana Personal Computer Security System product is designed to help separate and protect individual users' data on an IBM PC/XT or PC/AT workstation. When properly configured, the Cortana Personal Computer Security System may provide I&A, DAC, Object Reuse, and Audit mechanisms.

In order to provide these mechanisms, the administrator must configure the system to require a system password. By doing this, the administrator is assured that the proper date and time are entered for use in the audit log. The administrator must also prevent the users from performing certain actions. These include not allowing users of the workstation to have the system prompt, since this would allow them to introduce programs from the floppy drive that bypass the security mechanisms. Consequently, a custom menu must be set up for each user. These menus must prevent the user from having access to the following DOS commands:

DATE, TIME, DELETE, ASSIGN, and COMMAND

DATE and TIME should not be allowed to protect the integrity of the audit data. Not allowing users to execute the DELETE command will force the use of Shur-Lock's ZERO command to delete files, thus ensuring object reuse. ASSIGN and COMMAND must not be allowed because they provide the opportunity for users to introduce programs from the floppy disk drive. Discretion should also be used by the system administrator in assigning the remainder of the DOS commands such that each user has access to only those commands needed to perform his function.

To ensure that users of the workstation cannot get access to the system prompt the following restrictions should also be observed:

1. COMMAND.COM should be secured, using the secured functions menu, such that the administrator is the only one who can execute it.

2. The administrator should not allow applications which do not capture a break sequence. Any program that terminates when a Control-C or Control-Break is pressed falls under this category, such as DOS' LINK command.

3. The administrator should not allow applications which circumvent DOS (e.g. Norton Utilities[1]). Such applications use direct BIOS calls rather than DOS calls and are able to access physical sectors on a disk, thus circumventing the Cortana Personal Computer Security System.

4. To prevent users from creating applications which can circumvent DOS, the administrator should not allow such things as assemblers, compilers, and interpreters.

The first restriction will cause compatibility problems with many applications. Any program that relies on COMMAND.COM to execute will no longer be able to execute due to insufficient access. The remainder of the restrictions can severely limit the number of applications the System Administrator can allow on the system. However, this is the only way the product can be operated in a trusted manner.

---

(1) Norton Utilities is a registered trademark of Peter Norton Computing, Inc.

PRODUCT TESTING

Test Procedures

Testing represents a significant portion of a sub-system evaluation. The testing performed was primarily functional in nature; the security relevant characteristics of the product were compared against the claims of the vendor. The functional test suite of this product focused upon the following features: I&A, DAC, Object Reuse, and Audit. These security relevant features were identified in the *System Administrator's Guide*.

This test suite consisted of several parts. The I&A mechanism was tested extensively, including attempts to subvert it and to bypass it entirely.

Object Reuse tests were performed. They consisted of creating and ZEROing files and searching for remains of the file's contents on the disk media. In addition, memory was scanned after a log off and a new user logged on.

The DAC mechanism was subjected to high level access decision testing, involving authorized as well as unauthorized accesses to objects protected by Shur-Lock's address translation mechanism. The DAC mechanism was also tested at a lower level. Specifically, attempts were made to bypass this mechanism using various disk utility programs.

The Audit mechanism underwent extensive testing consisting of attempts to subvert or bypass the mechanism itself, attempts to corrupt audit data, and an attempt to overflow the audit data storage area.

All tests were performed on both an IBM PC/AT and IBM PC/XT[1] operating under PC-DOS[2] version 3.1.

---

(1) The IBM PC/AT and IBM PC/XT were configured with a single floppy disk drive and a single fixed hard drive.

(2) PC-DOS is a registered trademark of the International Business Machines Corporation.

Test Results

The test results described below are oriented toward providing the evaluation team's conclusions concerning the strengths and weaknesses of each security feature provided by the Cortana Personal Computer Security System.

The Cortana Personal Computer Security System testing was made difficult because the product frequently "locked up" the PC. The team feels this is due to the configuration restriction securing COMMAND.COM. Because the Cortana Personal Computer Security System modifies the File Allocation Table as its protection mechanism, when the system "locked up", the hard disk was un-usable and had to be re-formatted.

Identification and Authentication

The I&A mechanism was found to function properly; no access was granted to the machine prior to entering all required I&A information. The information used by the I&A mechanism was, however, found to be accessible by any user through the use of a disk utility program. Such programs are prevented from being introduced onto the system by the proper configuration. Although not stored in plain text, the information was both modifiable and corruptible.

High Level Discretionary Access Control

The DAC mechanism was found to function properly at the interface. The team found no way to circumvent the mechanism when restricted to standard DOS function calls.

Low Level Discretionary Access Control

The team found that the DAC mechanism could be bypassed using disk utility programs. All files that are inaccessible from DOS are stored in plain text and are able to be retrieved, written, and corrupted. To operate the Cortana Personal Computer Security System in a secure environment, such programs must not be allowed on the protected system.

Object Reuse

The object reuse mechanism was found to function as stated in the documentation: RAM is cleared at logoff, including memory resident programs, and, when DELETE is disabled and ZERO enabled for all users, files were overwritten. This only applies to deletions by explicit user actions. Implicit deletions, such as deletions from within programs, are not overwritten upon deletion because they do not rely on DOS, but rather BIOS.[1]

Audit

The audit records were found to contain the following information: time, date, event type, and user name. With the configuration set to audit all events, audit records are created for login and logout attempts, DOS programs, security officer actions, attempted security violations, and DOS commands.

All audit records are kept on the hard disk in a history file that will hold audit records for the number of days specified in the configuration. Once the audit file is exhausted, the Cortana Personal Computer Security System begins overwriting audit records beginning with the oldest.

The team found that audit information could be damaged through the use of disk utility programs. However, because the audit data is not in plain text, the audit information is protected so that there is some assurance that intelligible changes will not be made.

---

(1) A Pascal "rewrite" falls under this category.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS NONE
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT DISTRIBUTION UNLIMITED
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-88/002	5. MONITORING ORGANIZATION REPORT NUMBER(S) S230,477
6a. NAME OF PERFORMING ORGANIZATION National Computer Security Center 6b. OFFICE SYMBOL (If applicable) C12	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
(U) Sub-system Evaluation Report on Cortana Systems Corporation, Cortana Personal Computer Security System, Version 1.21

12. PERSONAL AUTHOR(S)
Stephen F. Carlton, Donald N. Dasher, John W. Taylor

13a. TYPE OF REPORT	13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT

16. SUPPLEMENTARY NOTATION

17 COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	NCSC TCSEC Cortana Audit I&A DAC identification authentication object reuse

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Cortana Systems Corporation Cortana Personal Computer Security System Version 1.21 product was evaluated against identification and authentication, Discretionary Access Control, Object Reuse and audit requirements of the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985. The product is a software and hardware package which, when properly installed, provides assurance through the implementation of the features listed above on a PC/XT OR PC/AT.

This report documents the findings of the evaluation.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL LTC Lloyd D. Gary, USA	22b. TELEPHONE (Include Area Code) (301)859-4458 22c. OFFICE SYMBOL C/C12

DD Form 1473, JUN 86 *Previous editions are obsolete*